

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method for providing cryptographic functions to data packets below the network layer of a network stack and ~~transparent to the~~ ~~hidden from said~~ network layer, the method including the steps of:

intercepting ~~in the data link layer of said network stack,~~ ~~datagrams transferred between~~ ~~outbound to and inbound from [[the]]~~ ~~said~~ network layer and ~~an other layer below the network~~ layer, ~~said~~ datagrams being encapsulated by a header and a footer associated with ~~transfer~~ ~~between the network layer and said [[other]] data link~~ layer and having at least one encapsulated data packet;

decapsulating ~~said~~ datagrams by removing ~~said~~ header and ~~said~~ footer to retrieve ~~said~~ at least one encapsulated data packet;

examining ~~said~~ at least one encapsulated data packet and referencing a security policy to determine whether to process ~~said~~ at least one encapsulated data packet according to ~~said~~ security policy using ~~said~~ cryptographic functions;

if ~~said~~ at least one encapsulated data packet requires processing, modifying ~~said~~ at least one encapsulated data packet to provide ~~said~~ cryptographic functions; ~~[[and]]~~

~~preparing reconstructed~~ ~~reconstructing~~ ~~said~~ datagrams by re-encapsulating ~~said~~ at least one encapsulated data packet with ~~said~~ header and ~~said~~ footer for transmission along ~~said~~ network stack; and

~~providing~~ ~~said~~ reconstructed datagrams back to ~~said~~ data link layer for continued transmission along ~~said~~ network stack.

2. (original) The method of claim 1 wherein ~~said~~ data packet is an IP packet having a header, an address and data.

3. (original) The method of claim 1 wherein ~~said~~ step of modifying ~~said~~ data packet includes the further step of selecting an IPSec protocol.

4. (currently amended) The method of claim 1 wherein the step of examining said at least one encapsulated data packet further includes the steps of:

 checking header information of outbound data packets from said network layer to determine if processing applies; and

 checking header information of inbound packets to said network layer to determine if said data packets include cryptographic functions.

5. (currently amended) A system for processing data packets for secure communications between correspondents of said system by providing cryptographic functions to data packets below the network layer of a network stack and ~~transparent to the~~ hidden from said network layer, said system having:

 a packet interceptor in the data link layer of said network stack for intercepting datagrams transferred between outbound to and inbound from the network layer and an other layer below the network layer, said datagrams being encapsulated by a header and a footer associated with transfer between the network layer and said [[other]] data link layer and having at least one encapsulated data packet, said packet interceptor for decapsulating said datagrams by removing said header and said footer to retrieve said at least one encapsulated data packet, and said packet interceptor for preparing reconstructed reconstructing said datagrams by re-encapsulating said at least one data packet with said header and said footer for transmission along said network stack and for providing reconstructed datagrams back to said data link layer for continued transmission along said network stack;

 a security policy manager including at least one security policy storing processing rules for said data packets and for selecting at least one of said processing rules for said at least one encapsulated data packet according to said security policy; and

 a processing module for examining said at least one encapsulated data packet decapsulated by said packet interceptor, and if said at least one encapsulated data packet requires processing, modifying said at least one encapsulated data packet by selecting and applying said cryptographic functions thereto, said processing module being in communication with said security policy manager;

 wherein said datagrams are intercepted and examined in accordance with said processing rules.

6. (currently amended) The system of claim 5, wherein the packet interceptor is a software module located at the ~~data link layer of the network stack~~.
7. (original) The system of claim 6, wherein said software module is a driver included in a kernel of an operating system in computer readable medium of said system.
8. (previously presented) The system of claim 5, wherein the cryptographic functions are implemented using an IPsec protocol by said processing module.
9. (previously presented) The system of claim 5, wherein said secure communications between correspondents of said system are provided via a virtual private network.
10. (currently amended) A method for providing a cryptographic system for communication between correspondents in a communication network to data packets below the network layer of a network stack and hidden from said network layer, said method comprising the steps of:
providing in the data link layer, a security module in a computer readable medium at each of said respondents, said security module having:
a packet interceptor for intercepting datagrams transferred between outbound to and inbound from the network layer and an other layer below the network layer, said datagrams being encapsulated by a header and a footer associated with transfer between the network layer and said [[other]] data link layer and having at least one encapsulated data packet, said packet interceptor for decapsulating said datagrams by removing said header and said footer to retrieve said at least one encapsulated data packet, and said packet interceptor for preparing reconstructed reconstructing said datagrams by re-encapsulating said at least one data packet with said header and said footer for transmission along said network stack and for providing said reconstructed datagrams back to said data link layer for continued transmission along said network stack;
a security policy manager including at least one security policy storing processing rules for said data packets and for selecting at least one processing rule for said encapsulated data packet according to said security policy; and

a processing module for examining said at least one encapsulated data packet decapsulated by said packet interceptor, and if said at least one encapsulated data packet requires processing, modifying said at least one encapsulated data packet by selecting and applying cryptographic functions thereto, said processing module being in communication with said security policy manager;

examining in said data link layer, said data packets decapsulated by said packet interceptor outbound ~~from said correspondents~~ to said network layer to determine whether processing by said processing module is required; and

examining in said data link layer, said data packets decapsulated by said packet interceptor inbound ~~to said correspondents~~ from said network layer to determine whether processing by said processing module is required by checking whether said data packets include cryptographic functions.

11. (cancel)

12. (currently amended) A method according to claim [[11]] 1 wherein said datagrams are PPP datagrams.

13. (previously presented) A method according to claim 1, said at least one encapsulated data packet being an IP data packet.

14. (previously presented) A method according to claim 1 wherein said modifying comprises IPsec tunneling.

15. (previously presented) A method according to claim 1 wherein said referencing comprises reviewing a predetermined set of selectors being one or more of a destination IP address and a transport layer port.